“Securing your business”

Anders Askåsen
Product Manager for OpenIDM
World Wide Coverage

ForgeRock.com
Enterprise Open Source Software

ForgeRock Norway
ForgeRock USA
ForgeRock UK
ForgeRock France

Consulting partners
Training partners
Presence through partners
Business Model

✓ Subscription
  • Service Level Agreement
  • Sustaining
  • Research & Development

✓ Training
OpenIDM
Initiate - Validate - Perpetuate
The classics of IdM?

✓ Life cycle management of Identities…
  - Joiners/Movers/Leavers – Onboarding/Offboarding

✓ … and dealing with their physical and digital access and entitlements
  - Provisioning and de-provisioning to systems

✓ Keeping track of who did what, why and when?
  - Reporting and Auditing
Governing Principles

✓ Lightweight
  - JSON, small footprint, few dependencies

✓ Developer friendly
  - Consistent APIs, Favored components

✓ Modular
  - OSGi – Use and run only services needed.

✓ Flexible
  - Plenty of extension points and integration capabilities.
Modularity

✅ **Dynamic Updates** - Bundles can be installed, started, stopped, updated, and uninstalled without bringing down the whole system.

✅ **Reduced Complexity**

  - The internal components are bundles, they hide their internals from other bundles and communicate through well defined services.
  - Hiding internals means more freedom to change later.

✅ **Simple, Small, Easy, Lazy, Versioning and Fast**

  - [http://www.osgi.org/About/WhyOSGi](http://www.osgi.org/About/WhyOSGi)
Provisioning Service

✓ Leverages the OpenICF framework for integration and connectivity with resources.

✓ Exposes capabilities to
  • Create, Update, Rename, Delete
  • Search
  • Ability to execute scripts
Discovery Service

User: John Doe

OpenIDM Virtual Identity

- DB: jd1234
- Unix: jdoe
- AD: cn=john.doe,ou=people,o=corp
- CSV File: John;Doe;
Identity Management related data is stored as Managed Objects.

Managed objects are stored by OpenIDM in its data store.

All managed objects are JSON-based data structures.

System Accounts are stored as System Objects.
Outbound Services

- Outbound Integration
  - Email Notifications
  - REST calls
- Information can be routed to any type of store (CSV, RDBMS, web services etc)
- Reporting Engines and Business Intelligence solutions can provide reports – OpenIDM provides the data.
- Fully configurable format on what to publish and when
Password Management

- Capability to synchronize passwords to integrated resources
- Intercept password changes natively on OpenDJ and ActiveDirectory via plug-ins.
- Supports password changes and resets according to password policy.
- Password resets using challenge questions
Business Logic and Rules

- By design pluggable to enable various languages such as Groovy, Ruby, JavaScript, Python etc
- Initially only JavaScript is supported but also allows call outs to Java methods or REST web services.
- Groovy “might” be next plug…
Product scope & vision

Identities
Accounts
Roles & Groups
Other objects
Hierarchy & Inheritance
Organizations
Policies & Rules

Life Cycle Management
Reporting
OSGi
Workflow
JSON
BPMN2
Audit & compliance
Password synchronization
SPML
Account Discovery & Reconciliation
Enterprise provisioning
OpenIDM
REGIST
Self-Service
Approvals
Certification
Auditing

OpenICF Framework
Open Standards
Support for .NET & Java
et cetera

ForgeRock
OpenDJ
Attachmate
IBM
Oracle
Microsoft
et cetera
Lets go in depth…

External Services

OSGi Core Services
Functional Overview

✓ Workflow and Business Process support
✓ Audit & Event publisher
  • Provides logging capabilities that external reporting engine can leverage.
✓ Provisioner Service
  • Exposes CRUD capabilities via REST.
✓ Discovery Service
  • Provides Reconciliation and Synchronization
✓ Outbound Service
  • Email notifications
  • Outbound REST
Typical Use-Cases

- HR (or authoritative source) driven provisioning
- Orphan accounts report (using external reporting engine) and cleansing
- Password Synchronization
- Synchronize identity data between resources.
- Basic CRUD via RESTful API for custom UIs.
Self-Service Registration
Change Password

New password
Please enter your new password in the fields below to change your password.

*Password ******

*Retype you password ******

Update my new password  Close
OpenIDM Subscription

OpenIDM:
1) Number of users
2) Number of connectors (and description)
3) A brief description of the scope of the IDM deployment
4) Type(s) of subscription (PoC, Build, Production):
5) Required response level from 24x7 2h to 8x5 Nxt day:
6) Overview of deployment project and timelines
Customers

(provided under NDA)
Customers

AKADEMISKA HUS

NSB

Universität Konstanz

Vodafone

OSLO VPS
Case-Study: Akademiska Hus

- Managing ca 3000 identities plus consultants/contractors.
- Biggest Real-estate company in Sweden managing properties worth over 50 billion SEK.
- Migration case from Sun IdM and Sun DSEE to OpenIDM and OpenDJ.
  - Synchronizing identities in AD and OpenDJ
  - Password Sync in AD and OpenDJ
Case-Study: NSB

- Managing ca 6000 identities plus consultants/contractors.
- 52 million journeys in Norway. 2 million in Sweden
- Phase 1 includes Identity Life-Cycle with provisioning driven by authoritative source (SAP HR) to AD
- Phase 2 provisioning to LDAP and Cloud provisioning to Office365.
Case-Study: VPS

- Managing ca 12,000 identities, customer exposing and critical to their core business
- Manages assets worth 383 Billion NOK.
- OpenIDM ensures the life-cycle of identities and provisions the correct authorizations in Tivoli Access Manager and IBM RACF.
- Password Resets for End Users
## Current Connectors

<table>
<thead>
<tr>
<th>Current Connectors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory (.net)</td>
</tr>
<tr>
<td>Database Table (db)</td>
</tr>
<tr>
<td>Scripted SQL (db)</td>
</tr>
<tr>
<td>DB2 (db)</td>
</tr>
<tr>
<td>MySQL (db)</td>
</tr>
<tr>
<td>Oracle (db)</td>
</tr>
<tr>
<td>MS SQL (db)</td>
</tr>
<tr>
<td>LDAP (ldap)</td>
</tr>
<tr>
<td>Exchange (.net)</td>
</tr>
<tr>
<td>SPMLv2 (Webservices)</td>
</tr>
<tr>
<td>RACF (mainframe)</td>
</tr>
<tr>
<td>Web TimeSheet (cloud)</td>
</tr>
<tr>
<td>Google Apps (cloud)</td>
</tr>
</tbody>
</table>
OpenICF Roadmap

Q3-Q4, 2011

Phase 1
Features
- OSGi Integration
- Connector Archetype
- OpenICF Documentation
  - Enhanced TAM
  - CSV ActiveSync
  - Scripted SQL

Core Framework for provisioning

2012

Phase 2
Features
- Enhanced Exception and Error handling
- HTTP Protocol support for Connector Server
- Optional MVCC Support
  - SharePoint
  - SAP HR
  - SAP R/3
  - SCIM connector
  - SalesForce.COM

FrameWork Improvements

2013

Phase 3
Features
- Unified Query Language
- PowerShell Support
  - Lotus Notes
  - Scripted REST connector
  - Top 10 Cloud Apps

Unified Query Language
3rd Party Connectivity

- IBM-RACF
- CA-ACF2
- CA-Top Secret
- IBM-i5
- Salesforce CRM
- SAP ECC
- Solaris
- Linux RED HAT
- HP Tandem
- HP-UX
- HP OpenVMS
Roadmap
Roadmap Summary

Q1, 2011

Milestone 1
Features
• Core Architecture based on OSGi
• Flexible Repository
• REST API supporting CRUD
• Connectors
  - Enhanced TAM
  - FlatFile ActiveSync
  - Scripted SQL

✓

Core Framework for provisioning

Q2, 2011

Milestone 2
Features
• Reconciliation and Discovery Engine
• Logging
• Bulk operations
• JavaScript driven Rules
• JDBC Repository Module

✓

Discovery and Reconciliation Engine

Q4, 2011

Release 2.0
Features
• Bi-directional unified Links
• Password Synchronization
• Reporting & auditing enhancements
• Authentication & Authorization
• JavaScript Debugger
• Resource Configuration Wizard
• Embedded BPMN 2.0 Workflow (Experimental)

✓✓✓

Core Identity Management system
Roadmap Summary

~Q3, 2012

Release 2.1
Features
• Workflow and Business Process support
• Improvements to Reconciliation
• JMX Monitoring
• Deferred Tasks
• Aggregated View
• End User User Dashboard

Workflow and Business Processes

~Q4, 2012

Release 2.2
Features
• Role Based Provisioning
• Organizations
• Administrative UI

Role Based Provisioning

~Q1, 2013

Release 2.3
Features
• Enhanced Administration UI
• Access Certification
• Role Engineering
• SoD Policy Engine
• Asynchronous Mappings

Access Certification & Compliance